Electronic Colloquium on Computational Complexity, Comment 1 on Report No. 029 (2001)

COMMENT ON TR01-29: A NOTE ON THE SUBGROUP MEMBERSHIP PROBLEM FOR $\mathrm{PSL}(2, p)$

DENIS XAVIER CHARLES

ABSTRACT. We use a classification theorem of Dickson, to show that the subgroup membership problem for $\mathrm{PSL}(2, p^f)$ is in $\mathrm{NP} \cap \mathrm{coNP}$.

1. Dickson's Theorem

In his study of Linear groups [DL58], Dickson completely classified all the subgroups of $\mathrm{PSL}(2, p^f)$ (the quotient of the group of 2×2 matrices with entries in $\mathrm{GF}[p^f]$ of determinant 1, by its center). We can use this theorem to show that the subgroup membership problem for $\mathrm{PSL}(2, p^f)$ is in $\mathrm{NP} \cap \mathrm{coNP}$. Specifically if we can show that the factor groups of composition series of these groups are not isomorphic to the exceptional family of simple groups then the membership problem for $\mathrm{PSL}(2, p^f)$ can be decided in $\mathrm{NP} \cap \mathrm{coNP}$ (see [CD01]). See Huppert's book [Hup67] (Hauptsatz 8.27, p. 213) for the version of the theorem that we will use.

Theorem 1.1 (Dickson). *The subgroups of* $\mathrm{PSL}(2, p^f)$ *are isomorphic to one of the following families of groups:*

1. *Elementary abelian p-groups;*
2. *Cyclic groups of order z, where z is a divisor of $\frac{p^f \pm 1}{k}$ and $k = (p^f - 1, 2)$;*
3. *Dihedral group of order $2z$, where z is as defined in (2);*
4. *Alternating group A_4 this can occur only for $p > 2$ or when $p = 2$ and $f \equiv 0 \mod 2$;*
5. *Symmetric group S_4 this can occur only if $p^{2f} \equiv 1 \mod 16$.*
6. *Alternating group A_5 for $p = 5$ or $p^{2f} \equiv 1 \mod 5$;*
7. *A semidirect product of an elementary abelian group of order p^m with a cyclic group of order t, where t is a divisor of $(p^m - 1, p^f - 1)$;*
8. *The group $\mathrm{PSL}(2, p^m)$ for m a divisor of f, or the group $\mathrm{PGL}(2, p^m)$ for $2m$ a divisor of f.*

Now we need to check that none of these families can have subgroups for which the exceptional groups occur as factor groups of composition series. This is easily done. Groups (1) and (2) are abelian so we can eliminate them. The dihedral groups, A_4, S_4 and the group family (7) are all solvable so again they can be excluded. A_5 is simple. Finally $\mathrm{PGL}(2, p^m)$ has $\mathrm{PSL}(2, p^m)$ sitting inside it as a maximal normal subgroup of index 2 if p is odd and if $p = 2$, then $\mathrm{PSL}(2, p^f) = \mathrm{PGL}(2, p^f)$. Thus the exceptional family of groups namely the Suzuki groups, the projective special unitary groups and the Ree groups do not occur as factor groups of composition series of any subgroup of $\mathrm{PSL}(2, p^f)$. Thus we have as a corollary (see [CD01]):

Corollary 1.2. *The subgroup membership problem for* $\mathrm{PSL}(2, p^f)$ *is in* $\mathrm{NP} \cap \mathrm{coNP}$.

Acknowledgements: I would like to thank Prof. Martin Isaacs for pointing out Dickson's work.

References

[CD01] Charles, Denis; *A note on the subgroup membership problem*, ECCC Technical report, TR01-29, 2001.

[DL58] Dickson, Leonard E.; *Linear Groups: With an exposition of the Galois field theory*, Dover Publications, New-York, 1958.

[Hup67] Huppert, Bertram; *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967.

Date: 10 Dec 2001.

Department of Computer Science, University of Wisconsin-Madison, Madison, WI - 53706, e-mail: cdx@cs.wisc.edu.

ISSN 1433-8092